# On digit patterns in expansions of rational numbers with prime denominator

Igor E. Shparlinski
Department of Computing, Macquarie University
Sydney, NSW 2109, Australia
igor.shparlinski@mq.edu.au

Wolfgang Steiner
LIAFA, CNRS, Université Paris Diderot – Paris 7
Case 7014, 75205 Paris Cedex 13, France
steiner@liafa.univ-paris-diderot.fr

March 4, 2013

**Abstract**

We show that, for any fixed $\varepsilon > 0$ and almost all primes $p$, the $g$-ary expansion of any fraction $m/p$ with $\gcd(m, p) = 1$ contains almost all $g$-ary strings of length $k < (5/24-\varepsilon) \log_g p$. This complements a result of J. Bourgain, S. V. Konyagin, and I. E. Shparlinski that asserts that, for almost all primes, all $g$-ary strings of length $k < (41/504-\varepsilon) \log_g p$ occur in the $g$-ary expansion of $m/p$.

## 1 Introduction

Let us fix some integer $g \geq 2$. It is well-known that if $\gcd(n, gm) = 1$ then the $g$-ary expansion of the rational fractions $m/n$ is purely periodic with period $t_n$, which is independent of $m$ and equals the multiplicative order of $g$ modulo $n$, see [9]. In the series of works [3, 8, 9], the distribution of digit patterns in such expansions has been studied. In particular, for positive integers $k$ and $m < n$ with $\gcd(n, gm) = 1$, we denote by $T_{m,n}(k)$ the number

of distinct $g$-ary strings $(d_1, \ldots, d_k) \in \{0, 1, \ldots, g-1\}^k$ that occur among the first $t_n$ trings $(\delta_r, \ldots, \delta_{r+k-1})$, $r = 1, \ldots, t_n$, from the $g$-ary expansion

$$\frac{m}{n} = \sum_{r=1}^{\infty} \delta_r g^{-r}, \quad \delta_r \in \{0, 1, \ldots, g-1\}. \tag{1}$$

Motivated by applications to pseudorandom number generators, see [1], we are interested in describing the conditions under which $T_{m,n}(k)$ is close to its trivial upper bound

$$T_{m,n}(k) \le \min\{t_n, g^k\}.$$

Since $t_n \le n$, it is clear that only values $k \le \lceil \log_g n \rceil$ are of interest. It has been shown in [8, Theorem 11.1] that, for any fixed $\varepsilon > 0$ and for almost all primes $p$ (that is, for all but $o(x/\log x)$ primes $p \le x$), we have $T_{m,p}(k) = g^k$, provided that $k \le (3/37 - \varepsilon) \log_g p$. The coefficient $3/37$ has been increased up to $41/504$ in [3, Corollary 8]. Here we show that, for almost all primes $p$, we have $T_{m,p}(k) = (1 + o(1))g^k$ for much larger string lengths $k$.

**Theorem 1.** *For any fixed $\varepsilon > 0$, for almost all primes $p$, we have*

$$T_{m,p}(k) = (1 + o(1))g^k$$

*as $p \to \infty$, provided that $k \le (5/24 - \varepsilon) \log_g p$.*

Our arguments depend on the reduction of the problem to the study of intersections of intervals and multiplicative groups modulo $p$ generated by $g$, that has been established in [8]. In turn, the question about the intersections of intervals and subgroups in residue rings has been studied in a number of works [3, 4, 8]. In particular, the results of [3, Corollary 8] and [8, Theorem 11.1] are based on estimates of the length of the longest interval that is not hit by a subgroup of the multplicative group $\mathbb{F}_p^*$ of the field $\mathbb{F}_p$ of $p$ elements. To prove Theorem 1, we use the results and ideas of [3] to estimate the total number of intervals of a given length that do not intersect a given subgroup of $\mathbb{F}_p^*$.

# 2 Multiplicative Orders

We recall the following well-known implication of the classical result of [5].

**Lemma 2.** *For almost all primes $p$, the multiplicative order $t$ of $g$ modulo $p$ satisfies $t > p^{1/2}$.*

# 3 Bounds of Some Exponential Sums

Let $p$ be prime and let $\mathcal{G} \subseteq \mathbb{F}_p^*$ be a subgroup of order $t$, where $\mathbb{F}_p$ is a finite field of $p$ elements.

We denote

$$\mathbf{e}_p(z) = \exp(2\pi i z/p)$$

and define exponential sums

$$S_\lambda(p;\mathcal{G}) = \sum_{v\in\mathcal{G}} \mathbf{e}_p(\lambda v).$$

Using [6, Lemma 3] (see also [8, Lemma 3.3]) if $t < p^{2/3}$, and the well known bounds

$$|S_\lambda(p;\mathcal{G})| \le p^{1/2} \quad \text{and} \quad \sum_{\lambda\in\mathbb{F}_p^*} |S_\lambda(p;\mathcal{G})|^2 \le pt$$

(see [8, Equations (3.4) and (3.15)]) if $t \ge p^{2/3}$, we derive:

**Lemma 3.** *For any prime $p$ and a subgroup $\mathcal{G} \subseteq \mathbb{F}_p^*$ of order $t$, we have*

$$\sum_{\lambda\in\mathbb{F}_p^*} |S_\lambda(p;\mathcal{G})|^4 \ll pt^{5/2}.$$

# 4 Intervals Avoiding Subgroups

As before, let $p$ be prime and let $\mathcal{G} \subseteq \mathbb{F}_p^*$ be a subgroup of order $t$.

Let $\mathcal{U}(p;\mathcal{G},H)$ be the set of $u \in \mathbb{F}_p$ such the congruence

$$v \equiv u + x \pmod p, \qquad v \in \mathcal{G},\ 0 \le x < H,$$

has no solution.

**Lemma 4.** *Assume that $\mathcal{G}$ is of order $t > p^{1/2}$. Then, for any fixed integer $\nu \ge 1$, we have*

$$\#\mathcal{U}(p;\mathcal{G},H) \le p^{2-1/4(\nu+1)+o(1)} H^{-1/2} t^{-5/4+(2\nu+1)/4\nu(\nu+1)} + p^{5/2-1/2\nu+o(1)} H^{-1} t^{-5/4+1/2\nu}.$$

*Proof.* Let us fix some $\varepsilon > 0$. We put

$$s = \left\lceil \frac{3}{2}(1+\varepsilon^{-1}) \right\rceil, \qquad h = \left\lceil p^{1+\varepsilon}/H \right\rceil, \qquad Z = \lceil H/s \rceil .$$

We can assume that $h < p/2$, as otherwise the bound is trivial (for example, it follows immediately from the bound of Heath-Brown and Konyagin [6, Theorem 1]). Obviously

$$\mathcal{U}(p; \mathcal{G}, H) \subseteq \mathcal{W}_s(p; \mathcal{G}, Z), \tag{2}$$

where $\mathcal{W}_s(p; \mathcal{G}, Z)$ is the set of $u \in \mathbb{F}_p$ such the congruence

$$v \equiv u + x_1 + \ldots + x_s \pmod{p}, \quad v \in \mathcal{G}, \quad 0 \le x_1, \ldots, x_s < Z, \tag{3}$$

has no solution.

For the number $Q_s(p; \mathcal{G}, Z, u)$ of solutions to the congruence (3), exactly as in the proof of [8, Lemma 7.1], we obtain

$$Q_s(p; \mathcal{G}, Z, u) = \frac{1}{p} \sum_{|a|<p/2} \mathbf{e}_p(-au) \left( \sum_{0 \le x < Z} \mathbf{e}_p(ax) \right)^s S_a(p; \mathcal{G}).$$

where the sums $S_a(p; \mathcal{G})$ are defined in Section 3.

Separating the term $tZ^s p^{-1}$ corresponding to $a = 0$ and summing over all $u \in \mathcal{W}_s(p; \mathcal{G}, Z)$ yields

$$0 = \sum_{u \in \mathcal{W}_s(p;\mathcal{G},Z)} Q_s(p; \mathcal{G}, Z, u) \ge \frac{tWZ^s}{p} - \frac{\sigma}{p},$$

where

$$W = \#\mathcal{W}_s(p; \mathcal{G}, Z)$$

and

$$\sigma = \sum_{1 \le |a| < p/2} \left| \sum_{u \in \mathcal{W}_s(p;\mathcal{G},Z)} \mathbf{e}_p(au) \right| \left| \sum_{0 \le x < Z} \mathbf{e}_p(ax) \right|^s |S_a(p; \mathcal{G})| .$$

Using the Cauchy inequality, and then the orthogonality relation for exponential functions, we obtain

$$\sigma^2 \le \sum_{1\le|a|<p/2} \left| \sum_{u\in\mathcal{W}_s(p;\mathcal{G},Z)} \mathbf{e}_p(au) \right|^2 \sum_{1\le|a|<p/2} \left| \sum_{0\le x<Z} \mathbf{e}_p(ax) \right|^{2s} |S_a(p;\mathcal{G})|^2$$
$$\le pW \sum_{1\le|a|<p/2} \left| \sum_{0\le x<Z} \mathbf{e}_p(ax) \right|^{2s} |S_a(p;\mathcal{G})|^2 .$$

Hence

$$W \le \frac{p}{t^2 Z^{2s}} \Sigma, \tag{4}$$

where

$$\Sigma = \sum_{1\le|a|<p/2} \left| \sum_{0\le x<Z} \mathbf{e}_p(ax) \right|^{2s} |S_a(p;\mathcal{G})|^2 .$$

Following the idea of the proof of [8, Lemma 7.1], we write

$$\Sigma = \Sigma_1 + \Sigma_2, \tag{5}$$

where

$$\Sigma_1 = \sum_{1\le|a|\le h} \left| \sum_{0\le x<Z} \mathbf{e}_p(ax) \right|^{2s} |S_a(p;\mathcal{G})|^2 ,$$
$$\Sigma_2 = \sum_{h<|a|<p/2} \left| \sum_{0\le x<Z} \mathbf{e}_p(ax) \right|^{2s} |S_a(p;\mathcal{G})|^2 .$$

For $1 \le |a| \le h$, we use the trivial estimate

$$\left| \sum_{0\le x<Z} \mathbf{e}_p(ax) \right| \le Z$$

and derive

$$\Sigma_1 \le Z^{2s} \sum_{1\le|a|\le h} |S_a(p;\mathcal{G})|^2 = \frac{Z^{2s}}{t} \sum_{1\le|a|\le h} \sum_{w\in\mathcal{G}} |S_{aw}(p;\mathcal{G})|^2$$
$$= \frac{Z^{2s}}{t} \sum_{\lambda\in\mathbb{F}_p^*} M_\lambda(p;\mathcal{G},h)\ |S_\lambda(p;\mathcal{G})|^2 ,$$

where $M_\lambda(p; \mathcal{G}, h)$ denotes the number of solutions to the congruence

$$\lambda \equiv aw \pmod p, \quad 1 \le |a| \le h, \quad w \in \mathcal{G}.$$

Hence, by the Cauchy inequality

$$\Sigma_1 \le \frac{Z^{2s}}{t} \left( \sum_{\lambda \in \mathbb{F}_p^*} M_\lambda(p; \mathcal{G}, h)^2 \right)^{1/2} \left( \sum_{\lambda \in \mathbb{F}_p^*} |S_\lambda(p; \mathcal{G})|^4 \right)^{1/2}.$$

As in [3, Section 3.3], we have

$$\sum_{\lambda \in \mathbb{F}_p^*} M_\lambda(p; \mathcal{G}, h)^2 \le tN(p; \mathcal{G}, h),$$

where $N(p; \mathcal{G}, h)$ is the number of solutions of the congruence

$$ux \equiv y \pmod p, \quad 0 < |x|, |y| \le h, \quad u \in \mathcal{G}.$$

Therefore,

$$\Sigma_1 \le \frac{Z^{2s}}{t^{1/2}} N(p; \mathcal{G}, h)^{1/2} \left( \sum_{\lambda \in \mathbb{F}_p^*} |S_\lambda(p; \mathcal{G})|^4 \right)^{1/2}. \tag{6}$$

It is shown in [3, Theorem 1] that if $t \ge p^{1/2}$ then for any fixed integer $\nu$ and any positive number $h$, we have

$$N(p; \mathcal{G}, h) \le ht^{(2\nu+1)/2\nu(\nu+1)} p^{-1/2(\nu+1)+o(1)} + h^2 t^{1/\nu} p^{-1/\nu+o(1)}. \tag{7}$$

Therefore, using Lemma 3 and the bound (7) we derive from (6) that

$$\Sigma_1 \le p^{1/2} t^{3/4} Z^{2s} \left( h^{1/2} t^{(2\nu+1)/4\nu(\nu+1)} p^{-1/4(\nu+1)+o(1)} + ht^{1/2\nu} p^{-1/2\nu+o(1)} \right). \tag{8}$$

If $h < |a| < p/2$, then we use the bound

$$\sum_{0 \le x < Z} \mathbf{e}_p(ax) \ll \frac{p}{|a|},$$

see [7, Bound (8.6)]. From the trivial bound

$$|S_a(p; \mathcal{G})| \le t,$$

recalling the choice of $h$, we obtain

$$\Sigma_2 \ll \sum_{h<|a|<p/2} \left(\frac{p}{|a|}\right)^{2s} t^2 \ll t^2 \frac{p^{2s}}{h^{2s-1}} \ll t^2 \frac{Z^{2s}h}{p^{2s\varepsilon}} \le \frac{Z^{2s}p^3}{p^{2s\varepsilon}} \ll Z^{2s},$$

as $2s\varepsilon > 3$ for our choice of $s$. Thus the bound on $\Sigma_2$ is dominated by the bound (8) on $\Sigma_1$. Using (4) and (5), we obtain

$$W \le p^{3/2}t^{-5/4}\big(h^{1/2}t^{(2\nu+1)/4\nu(\nu+1)}p^{-1/4(\nu+1)+o(1)} + ht^{1/2\nu}p^{-1/2\nu+o(1)}\big).$$

Recalling (2), the choice of $h$ and that $\varepsilon$ is arbitrary, after simple calculations, we obtain the result. □

**Corollary 5.** *Assume that $\mathcal{G}$ is of order $t > p^{1/2}$. Then for any $\varepsilon > 0$ and*

$$H \ge p^{19/24+\varepsilon}$$

*we have*

$$\#\mathcal{U}(p; \mathcal{G}, H) = o(p).$$

*Proof.* Since $t > p^{1/2}$, we have, for any fixed integer $\nu \ge 1$,

$$\#\mathcal{U}(p; \mathcal{G}, H) \le p^{11/8+1/8\nu(\nu+1)+o(1)}H^{-1/2} + p^{15/8-1/4\nu+o(1)}H^{-1}.$$

Taking $\nu = 2$ or $\nu = 3$, we conclude the proof. □

# 5 Proof of Theorem 1

By Lemma 2 it is enough to consider prime $p$ for which the multiplicative order $t$ of $g$ modulo $p$ satisfies $t > p^{1/2}$.

We now take a positive integer $k \le (5/24 - \varepsilon)\log_g p$ and consider the intervals $\big[\frac{D}{g^k}, \frac{D+1}{g^k}\big)$. As in the proof of [8, Theorem 11.1], we observe that, for any integer $\ell \ge 0$ and any $g$-ary string $(d_1, \ldots, d_k)$, we have $\delta_{\ell+i} = d_i$, $i = 1, \ldots, k$, if and only if

$$\frac{mg^\ell}{p} - \left\lfloor \frac{mg^\ell}{p} \right\rfloor \in \left[\frac{D}{g^k}, \frac{D+1}{g^k}\right),$$

where $D = d_1 g^{k-1} + d_2 g^{k-2} + \cdots + d_k$ and the $\delta_r$, $r = 1, 2, \ldots$, are defined by (1) with $n = p$. Thus, if a string $(d_1, \ldots, d_k)$ is not present in the $g$-ary expansion of $m/p$, then each interval $[u, u + H)$ with

$$u = \left\lceil \frac{D}{g^k} p \right\rceil, \ldots, \left\lfloor \frac{D + 1/2}{g^k} p \right\rfloor \quad \text{and} \quad H = \left\lfloor \frac{1}{2g^k} p \right\rfloor$$

contains no element of the conjugacy class $m\mathcal{G}_p$ of the group $\mathcal{G}_p$ generated by $g$ modulo $p$. Clearly, different strings $(d_1, \ldots, d_k)$ correspond to different intervals of the values of $u$, and each of them contains

$$\left\lceil \frac{D + 1/2}{g^k} p \right\rceil - \left\lceil \frac{D}{g^k} p \right\rceil \gg \frac{p}{g^k}$$

values of $u$. Therefore, the number of missing strings $(d_1, \ldots, d_k)$ satisfies

$$g^k - T_{m,p}(k) \ll \frac{g^k}{p} \#\mathcal{U}(p; \mathcal{G}_p, H).$$

Since $g^k \le p^{5/24-\varepsilon}$, we infer from Corollary 5 that $\#\mathcal{U}(p; \mathcal{G}_p, H) = o(p)$, which proves Theorem 1.

# 6 Composite Denominators

It is quite likely that one can also study $T_{m,n}(k)$ for almost all composite $n$ by supplementing the ideas of this work with those of [2] (to get an analogue of Lemma 3) and also using the result of [10] that gives an analogue of Lemma 2.

# Acknowledgements

The second author wishes to express his heartfelt thanks to the members of the Department of Computing of the Macquarie University for their hospitality during his stay as a visiting academic.

During the preparation of this work the first author was supported in part by the Australian Research Council Grant DP1092835.

# References


[1] L. Blum, M. Blum and M. Shub, 'A simple unpredictable pseudo-random number generator', *SIAM J. Comp.*, **15** (1986), 364–383.

[2] J. Bourgain, S. Konyagin, C. Pomerance and I. E. Shparlinski, 'On the smallest pseudopower', *Acta Arith.*, **140** (2009), 43–55.

[3] J. Bourgain, S. V. Konyagin and I. E. Shparlinski, 'Product sets of rationals, multiplicative translates of subgroups in residue rings and fixed points of the discrete logarithm', *Intern. Math. Res. Notices*, **2008** (2008), Article ID rnn090, 1–29. (Corrigenda: *Intern. Math. Res. Notices*, **2009** (2009), 3146–3147).

[4] J. Bourgain, S. V. Konyagin and I. E. Shparlinski, 'Distribution of elements of cosets of small subgroups and applications', *Intern. Math. Res. Notices*, **2012** (2012), Article ID rnn097, 1968-2009.

[5] P. Erdős and M. R. Murty, 'On the order of $a \pmod p$', *Proc. 5th Canadian Number Theory Association Conf.*, Amer. Math. Soc., Providence, RI, 1999, 87–97.

[6] D. R. Heath-Brown and S. V. Konyagin, 'New bounds for Gauss sums derived from $k$th powers, and for Heilbronn's exponential sum', *Quart. J. Math.*, **51** (2000), 221–235.

[7] H. Iwaniec and E. Kowalski, *Analytic number theory*, American Mathematical Society, Providence, RI, 2004.

[8] S. V. Konyagin and I. E. Shparlinski, *Character sums with exponential functions and their applications*, Cambridge Univ. Press, Cambridge, 1999.

[9] N. M. Korobov, 'On the distribution of digits in periodic fractions', *Matem. Sbornik*, 89 (1972), 654–670 (in Russian).

[10] P. Kurlberg and C. Pomerance, 'On the period of the linear congruential and power generators', *Acta Arith.*, **119** (2005), 149–169.